IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Matthew P. Duggan, *et al.*	§	Group Art Unit: 2132
	§	
	§	Examiner: Kim, Jung W.
Serial No.: 10/815,213	§	
	§	Atty Docket No.: AUS920040010US1
Filed: 03/31/2004	§	
	§	Customer No.: 34533
Title: Cross Domain Security Information Conversion	§	
	§	Confirmation No.: 7107

Mail Stop: Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPEAL BRIEF

Honorable Commissioner:

This is an Appeal Brief filed pursuant to 37 CFR § 41.37 in response to the Final Office Action of April 11, 2008 (hereinafter the "Office Action"), and pursuant to the Notice of Appeal filed July 10, 2008.

REAL PARTY IN INTEREST

The real party in interest in accordance with 37 CFR § 41.37(c)(1)(i) is the patent assignee, International Business Machines Corporation ("IBM"), a New York corporation having a place of business at Armonk, New York 10504.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences within the meaning of 37 CFR § 41.37(c)(1)(ii).

STATUS OF CLAIMS

Status of claims in accordance with 37 CFR § 41.37(c)(1)(iii): Twenty-eight (28) claims are filed in the original application in this case. Claims 1-28 are rejected in the Office Action. Claims 1-28 are on appeal.

STATUS OF AMENDMENTS

Status of amendments in accordance with 37 CFR § 41.37(c)(1)(iv): No amendments were submitted after final rejection. The claims as currently presented are included in the Appendix of Claims that accompanies this Appeal Brief.

SUMMARY OF CLAIMED SUBJECT MATTER

Appellants provide the following concise summary of the claimed subject matter according to 37 CFR § 41.37(c)(1)(v). This summary includes a concise explanation of the subject matter defined in each of the independent claims involved in the appeal and includes references to the specification by page and line number and to the drawings by elements. The three independent claims involved in this appeal are claims 1, 10, and 19. Claims 1 is a method claim. Claims 10 and 19 recite counterpart aspects of the method of claim 1. Claim 10 recites system aspects of the method of claim 1. Claim 19 recites computer program product aspects of the method of claim 1.

This summary also includes an explanation of the subject matter defined in dependent claims 3, 6, 12, 15, 21, and 24. Claim 3 is a method claim. Claims 12 and 21 recite counterpart aspects of the method of claim 3. Claim 12 recites system aspects of the method of claim 3. Claim 21 recites computer program product aspects of the method of claim 3. Claim 3 is a method claim. Claims 15 and 24 recite counterpart aspects of the method of claim 6. Claim 15 recites system aspects of the method of claim 6. Claim 24 recites computer program product aspects of the method of claim 6.

Claim 1 recites a method for cross domain security information conversion (page 12, lines 28-29; Figure 2). The method of claim 1 includes receiving from a system entity, in a security service, security information in a native format of a first security domain regarding a system entity having an identity in at least one security domain (page 12, line 30 – page 13, line 1; Figure 2, elements 202, 110, 102, and 212). The method of claim 1 also includes translating the security information to a canonical format for security information (page 15, lines 20-21; Figure 2, elements 204 and 214). The method of claim 1 also includes transforming the security information in the canonical format using a predefined mapping from the first security domain to a second security domain (page 19, lines 11-13; Figure 2, elements 206 and 214). The method of claim 1 also includes translating the transformed security information in the canonical format to a native format of the second security domain (page 24, lines 4-6; Figure 2, elements 208 and 216). The method of claim 1 also includes returning to the system entity the security information in the native format of the second security domain (page 24, lines 14-16; Figure 2, elements 210 and 218).

Claim 3 recites the method of claim 1 wherein receiving security information further comprises receiving a request for security information for the second security domain, wherein the request encapsulates the security information in a native format of a first security domain. (page 11, line 31 – page 12, line 2; Figure 1, elements 108 and 106).

Claim 6 recites the method of claim 1 wherein translating the security information in a native format of a first security domain to a canonical format is carried out through a procedural software function. (page 17, line 23-31; Figure 2, elements 204 and 214).

Claim 10 recites a system for cross domain security information conversion (page 12, lines 28-29; Figure 2). The system of claim 10 includes means for receiving from a system entity, in a security service, security information in a native format of a first security domain regarding a system entity having an identity in at least one security domain (page 12, line 30 – page 13, line 1; Figure 2, elements 202, 110, 102, and 212).

The system of claim 10 also includes means for translating the security information to a canonical format for security information (page 15, lines 20-21; Figure 2, elements 204 and 214). The system of claim 10 also includes means for transforming the security information in the canonical format using a predefined mapping from the first security domain to a second security domain (page 19, lines 11-13; Figure 2, elements 206 and 214). The system of claim 10 also includes means for translating the transformed security information in the canonical format to a native format of the second security domain (page 24, lines 4-6; Figure 2, elements 208 and 216). The system of claim 10 also includes means for returning to the system entity the security information in the native format of the second security domain (page 24, lines 14-16; Figure 2, elements 210 and 218).

Claim 12 recites the system of claim 10 wherein means for receiving security information further comprises means for receiving a request for security information for the second security domain, wherein the request encapsulates the security information in a native format of a first security domain. (page 11, line 31 – page 12, line 2; Figure 1, elements 108 and 106).

Claim 15 recites the system of claim 10 wherein means for translating the security information in a native format of a first security domain to a canonical format comprises a procedural software function. (page 17, line 23-31; Figure 2, elements 204 and 214).

Claim 19 recites a computer program product for cross domain security information conversion (page 12, lines 28-29; Figure 2). The computer program product of claim 19 includes a recording medium (page 6, lines 18-19). The computer program product of claim 19 also includes means, recorded on the recording medium, for receiving from a computer program product entity, in a security service, security information in a native format of a first security domain regarding a computer program product entity having an identity in at least one security domain (page 12, line 30 – page 13, line 1; Figure 2, elements 202, 110, 102, and 212). The computer program product of claim 19 also includes means, recorded on the recording medium, for translating the security

information to a canonical format for security information (page 15, lines 20-21; Figure 2, elements 204 and 214). The computer program product of claim 19 also includes means, recorded on the recording medium, for transforming the security information in the canonical format using a predefined mapping from the first security domain to a second security domain (page 19, lines 11-13; Figure 2, elements 206 and 214). The computer program product of claim 19 also includes means, recorded on the recording medium, for translating the transformed security information in the canonical format to a native format of the second security domain (page 24, lines 4-6; Figure 2, elements 208 and 216). The computer program product of claim 19 also includes means, recorded on the recording medium, for returning to the computer program product entity the security information in the native format of the second security domain (page 24, lines 14-16; Figure 2, elements 210 and 218).

Claim 21 recites the computer program product of claim 19 wherein means, recorded on the recording medium, for receiving security information further comprises means, recorded on the recording medium, for receiving a request for security information for the second security domain, wherein the request encapsulates the security information in a native format of a first security domain. (page 11, line 31 – page 12, line 2; Figure 1, elements 108 and 106).

Claim 24 recites the computer program product of claim 19 wherein means, recorded on the recording medium, for translating the security information in a native format of a first security domain to a canonical format comprises a procedural software function. (page 17, line 23-31; Figure 2, elements 204 and 214).

GROUNDS OF REJECTION

In accordance with 37 CFR § 41.37(c)(1)(vi), Appellants provide the following concise statement for each ground of rejection:

1. Claims 10-28 stand rejected under 35 U.S.C. § 101 on grounds that the claims

recite non-statutory subject matter.

2. Claims 1-6, 10-15, 19-24, and 27 stand rejected under 35 U.S.C. § 102(b) over Botz *et al.*, (U.S. Patent 6,981,043).

3. Claims 7-9, 16-18, 25-26, and 28 stand rejected for obviousness under 35 U.S.C. § 103(a) as being unpatentable over Botz in view of Bussler *et al.*, (U.S. Patent 7,072,898).

ARGUMENT

Appellants present the following argument pursuant to 37 CFR § 41.37(c)(1)(vii) regarding the ground of rejection on appeal in the present case.

Argument Regarding The First Ground Of Rejection On Appeal: Claims 10-28 Stand Rejected Under 35 U.S.C. § 101 On Grounds That The Claims Recite Non-statutory Subject Matter

Claims 10-28 stand rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. The Office Action at page 2, states:

> Claims 10-28 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. These claims do not restrict the claimed invention to statutory classes of invention. Rather, the specification defines computer program products embodied on a recording medium to encompass transmission media. (See Specification, pg. 6, line 22) Hence, these claims are limited to statutory subject matter.

That is, the Office Action takes the position that Appellants' usage of the term 'recording medium' in claims 19-28 renders Appellants' claims outside realm of statutory subject matter because 'recording medium' encompasses 'transmission medium.' As confirmed in the telephone conversation with Examiner Kim on December 12, 2007, claims 10-18 are rejected as non-statutory subject matter because the 'means' in the 'means for' limitations of claims 10-18 may include the 'recording medium' of claims 19-28. For the

reasons discussed below, Appellants' claims 19-28 that include 'recording medium' are statutory subject matter entitled to patent protection. As such, Appellants' claims 10-18 are also within the realm of statutory subject matter, and the rejection of Appellants' claim 10-28 under 35 U.S.C. § 101 should be withdrawn.

In asserting that Appellants' claims are directed toward non-statutory subject matter because 'recording medium' encompasses 'transmission medium,' the Office Action implies that Appellants' claims are directed toward non-statutory subject matter because a 'transmission medium' may be used to transfer signals. The current law regarding the patentability of signals is *In re Nuijten*, No. 06-1371 (Fed. Cir. 2007). In *Nuijten*, the Court held that a signal claimed as signal is not statutory subject matter eligible for patentability. Appellants note in the present application, however, that Appellants are not claiming a signal as a signal—rather, Appellants are claiming a computer program product that includes a recording medium on which suitable programming means may be recorded. In fact, the Court in *Nuijten* noted that the Board of Patent Appeals and Interferences ('BPAI') decided that a similar claiming pattern in *Nuijten* was directed toward statutory subject matter stating:

> Finally, Nuijten's allowed Claim 15 is directed to "[a] storage medium having stored thereon a signal with embedded supplemental data..."
>
> On appeal, the Board reversed the double-patenting rejections. As to Claim 15, it found that "[t]he storage medium in claim 15 nominally puts the claim into the statutory category of a 'manufacture'" and thus reversed the Examiner's § 101 rejection of that claim.

For the same reasons that the BPAI held that the claims in *Nuijten* directed toward storage medium having stored thereon a signal with embedded supplemental data, Appellants submit that claims 19-28 directed toward a computer program product that includes a recording medium on which suitable programming means may be recorded is also patentable under 35 U.S.C. § 101. As such, Appellants' claims 10-18 are also directed toward statutory subject matter.

Furthermore, Appellants noted that even though the term 'recording medium' encompasses the term 'transmission medium,' Appellants' original specification describes a 'transmission medium' as being a suitable recording medium for machine-readable information, which is used to embody the computer program product claimed in the present application. Nothing in the cited reference or any other language in the specification or the claims describes 'transmission media' as a signal or under any reasonable interpretation implies that Appellants are claiming a signal. In addition, Appellants note that the Fifth Edition of the Microsoft Computer Dictionary defines the term 'media' as "a physical material, such as paper, disk, and tape, used for storing computer-based information." One of ordinary skill in the art would therefore understand that 'transmission media' is a physical material and entitled to patent protection under 35 U.S.C. § 101 as an article of manufacture or a composition of matter. The rejections of claims 10-28 under 35 U.S.C. § 101 are improper, and should therefore be withdrawn. Appellants respectfully request reconsideration of claim 10-28.

Argument Regarding The Second Ground Of Rejection On Appeal: Claims 1-6, 10-15, 19-24, and 27 Are Rejected Under 35 U.S.C. §102(b) Over Botz

Claims 1-6, 10-15, 19-24, and 27 stand rejected under 35 U.S.C. § 102 as being anticipated by Botz, *et al.* (U.S. Patent No. 6,981,043). To anticipate claims 1-6, 10-15, 19-24, and 27 under 35 U.S.C. § 102, Botz must disclose each and every element and limitation recited in the claims of the present application.

Botz Does Not Disclose Each And Every Element Of The Claims Of The Present Application

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631. 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Independent claim 1 recites:

1. A method for cross domain security information conversion, the method comprising:

receiving from a system entity, in a security service, security information in a native format of a first security domain regarding a system entity having an identity in at least one security domain;

translating the security information to a canonical format for security information;

transforming the security information in the canonical format using a predefined mapping from the first security domain to a second security domain;

translating the transformed security information in the canonical format to a native format of the second security domain; and

returning to the system entity the security information in the native format of the second security domain.

As explained below, Botz does not disclose each and every element and limitation recited in the claims of the present application and therefore does not anticipate the claims of the present application.

Botz Does Not Disclose Receiving From A System Entity, In A Security Service, Security Information In A Native Format Of A First Security Domain And Returning To The System Entity The Security Information In The Native Format Of The Second Security Domain

The Office Action takes the position that Botz at column 14, lines 17-34, discloses: receiving from a system entity, in a security service, security information in a native format of a first security domain regarding a system entity having an identity in at least

one security domain and returning to the system entity the security information in the native format of the second security domain. Appellants respectfully note in response, however, that what Botz at column 14, lines 17-34, in fact discloses is:

> The identity mapping mechanism of the present invention provides an infrastructure for creating mappings between local user identities in different user registries on a network. In the preferred embodiment, a global identifier is created for each user, and each local user identity that corresponds to the global identifier is mapped to the global identifier. Once the relationship between the local user identities and the global identities is established, the infrastructure can then be used to determine from one local user identity a corresponding local user identity in a different user registry. The identity mapping mechanism thus allows user information in one environment to automatically retrieve user information in a different environment, thereby avoiding the necessity of the user remembering multiple usernames and passwords. Once a user it authorized to the network, and requests access to a resource, the security semantics for obtaining access to the resource may be satisfied by invoking the appropriate EIM APIs and submitting the appropriate security information.

That is, Botz, at column 14, lines 17-34, discloses a user identity mapping mechanism for creating mappings between user identities in different user registries on a network. Botz's user identity mapping mechanism that creates mappings between user identities in different user registries on a network, however, does not disclose receiving from a system entity, in a security service, security information in a native format of a first security domain regarding a system entity having an identity in at least one security domain and returning to the system entity the security information in the native format of the second security domain as claimed in the present application because Botz's user identity mapping mechanism operates exclusively within a *single* domain to correlate a user's local user identities stored in different user registries within the *single* domain. Botz at column 9, line 59, states that a domain "represents a logical division for managing user identities." Botz then goes on to describe how a global identifier for a user is used to map a user's local identity in a user registry within a domain to that user's local identity in a different user registry within the *same* domain. *See* Botz at column 9, line 59, through column 10, line 25, and Figure 14. That is, Botz discloses mapping user

identities within a single domain. Because Botz's user identity mapping mechanism operates exclusively within a single domain to correlate a user's local user identities stored in different user registries within the single domain, Botz does not disclose multiple domains. Without disclosing multiple domains, Botz cannot disclose a second security domain, as claimed in the present application. Because Botz does not disclose a second security domain, Botz does not disclose receiving security information in a native format of a first security domain and returns the security information in the native format of a second security domain as claimed in the present application. Because Botz does not disclose each and every element and limitation of Appellants' claims, Botz does not anticipate Appellants' claims, and the rejections under 35 U.S.C. § 102 should be withdrawn.

Botz Does Not Disclose Translating The Security Information To A Canonical Format For Security Information

The Office Action takes the position that Botz at column 9, lines 46-54 and Figure 10 discloses: translating the security information to a canonical format for security information and transforming the security information in the canonical format using a predefined mapping from the first security domain to a second security domain. Appellants respectfully note in response, however, that what Botz at column 9, lines 46-54, in fact discloses is:

> A global identifier is generated that corresponds to a user (step 1310). We assume for this example that this user has a first user identity in a first user registry, and a second user identity in a second user registry. The first user identity is mapped to the global identifier (step 1320). The second user identity is also mapped to the global identifier (step 1330). Because both local user identities are now mapped to a common global identifier, the mapping between these two local user identities can be easily determined

That is, Botz at column 9, lines 46-54, discloses mapping user identities in separate user registries to a single global identifier. Botz's mapping user identities in separate user registries to a single global identifier does not disclose translating the security information to a canonical format for security information and transforming the security information in the canonical format using a predefined mapping from the first security

domain to a second security domain, as claimed in the present application, because Botz's mapping is not translating, as claimed in the present application. As claimed in the present application, information is translated from one format to a canonical format. In the original specification, Appellants at page 15, line 31 – page 16, line 2, define a canonical format as a "data format for security information that is standardized for use in data transformations of security information." In contrast to security information that is translated from one format to a data format that is standardized for use in data transformations of security information, Botz discloses mapping. Botz discusses mapping as correlating multiple user identities in different environments to a single user. *See* Botz at column 5, lines 42-50. Correlating multiple user identities in different environments to a single user does not include translating security information from one format to a data format that is standardized for use in data transformations of security information. In fact, at no point in the reference does Botz discuss the topic of translating data formats or even mention the keyword "canonical." Without disclosing translating data formats, Botz does not disclose translating the security information to a canonical format for security information, as claimed in the present application. Because Botz does not disclose each and every element and limitation of Appellants' claims, Botz does not anticipate Appellants' claims, and the rejections under 35 U.S.C. § 102 should be withdrawn.

In Response To Office Action's 'Response to Arguments'

The Office Action responds to Appellants' previous arguments in a Response to Arguments section. The Office Action at page 2 states,

> A domain, as taught by Botz, does not define security divisions as claimed in Appellant's claims. Rather, the domain of Botz's invention defines general logical divisions ("The domain 1410 represents a logical division for managing user identities. A domain 1410 can be a company, a division within a company, a building within a division, or any other division that indicates a physical relationship. Furthermore, a domain 1410 can be strictly logical divisions, such as hourly employees and salaried employees," col. 9:60-65) As outlined in the rejections below, Appellant's claimed recitation of a native format of a first and second

> security domains are in fact suggested by the various environments which utilize different security protocols (see fig. 10). As taught by Botz, each local user identity on their respective security environments is mapped to the other local user identities via an enterprise identifier. (col. 9:46-54) For these reasons, Botz anticipates claims 1-6, 10-15, 19-24, and 27.

Appellants understand this statement from the Office Action as an assertion that Botz's domains are not security domains, as claimed in the present application, but Botz's various environments, disclosed in Fig. 10, suggest security domains, as claimed in the present application. Appellants respectfully note in response, however, that Botz at column 7, lines 35-40, discusses the 'various environments' of Fig. 10, stating:

> Now we see from FIG. 10 how the preferred embodiments allow the system administrator to correlate the single global identifier 1010 to several different local user identities in different user registries. We assume that this user has a local user identity JohnASmith in the AS400-1 registry

That is, Botz's 'various environments' are user registries. Botz's user registries are not security domains, as claimed in the present application. In the original specification at page 8, line 29, Appellants describe a security domain, stating that "a security domain represents a single unit of security administration and trust." Furthermore, Appellants define trust as "the characteristic that one system entity is willing to rely upon a second entity to execute actions or to make assertions about system entities or scopes." *See* Appellants' original specification at page 8, lines 30-31. In contrast to a single unit of security administration and trust, Botz defines a user registry as "a list of users and information, such as a user ID and password, that are used to authenticate a user when the user requests access to the network." *See* Botz at column 1, lines 31-33. That is, Botz discloses different locations on a network that contain lists of users and security information that is used to authenticate a user when the user requests access to the network. A location containing lists of users and security information that can be used to authenticate a user when the user requests access to the network discloses different locations containing security information – not security domains representing a single unit of security administration and trust. Because Botz does not disclose each and every

element and limitation of Appellants' claims, Botz does not anticipate Appellants' claims, and the rejections under 35 U.S.C. § 102 should be withdrawn.

Botz Does Not Enable Each and Every Element Of The Claims Of The Present Application

Not only must Botz disclose each and every element of the claims of the present application within the meaning of *Verdegaal* in order to anticipate Appellants' claims, but also Botz must be an enabling disclosure of each and every element of the claims of the present application within the meaning of *In re Hoeksema*. In *Hoeksema*, the claims were rejected because an earlier patent disclosed a structural similarity to the Appellant's chemical compound. The court in *Hoeksema* stated: "We think it is sound law, consistent with the public policy underlying our patent law, that before any publication can amount to a statutory bar to the grant of a patent, its disclosure must be such that a skilled artisan could take its teachings in combination with his own knowledge of the particular art and be in possession of the invention." *In re Hoeksema*, 399 F.2d 269, 273, 158 USPQ 596, 600 (CCPA 1968). The meaning of *Hoeksema* for the present case is that unless Botz places Appellants' claims in the possession of a person of ordinary skill in the art, Botz is legally insufficient to anticipate Appellants' claims under 35 U.S.C. § 102. As explained above, Botz does not disclose each and every element and limitation of independent claim 1 of the present application. Because Botz does not disclose each and every element, Botz cannot possibly place the elements and limitations of the independent claims in the possession of a person of ordinary skill in the art. Botz cannot, therefore, anticipate claim 1 of the present application.

Relations Among Claims

Independent claims 10 and 19 are system and computer program product claims for cross domain security information conversion corresponding to independent method claim 1. For the same reasons that Botz does not disclose a method for cross domain security information conversion, Botz also does not disclose a system and computer program product for cross domain security domain security information conversion corresponding

to independent claims 10 and 19. Independent claims 10 and 19 are therefore patentable and should be allowed.

Claims 2-6, 11-15, 20-24, and 27 depend from independent claims 1, 10, and 19. Each dependent claim includes all of the limitations of the independent claim from which it depends. Because Botz does not disclose or enable each and every element of the independent claims, Botz does not disclose or enable each and every element of the dependent claims of the present application. As such, claims 2-6, 11-15, 20-24, and 27 are also patentable and should be allowed.

Botz Does Not Disclose Each And Every Element Of The Dependent Claims Of The Present Application

In addition to the fact that Botz does not disclose each and every element and limitation of the claim 1 of the present application, there is another reason that Botz does not disclose each and every element and limitation of the dependent claims of the present application – that is, Botz itself does not disclose each and every element and limitation of the dependent claims. Consider dependent claims 3 and 6 as examples.

The Office Action takes the position that Botz at column 14, lines 23-34 discloses the following limitation recited in dependent claim 3 of the present application: receiving security information further comprises receiving a request for security information for the second security domain, wherein the request encapsulates the security information in a native format of a first security domain. Appellants note in response, however, that what Botz at column 14, lines 23-34 in fact discloses is:

> Once the relationship between the local user identities and the global identities is established, the infrastructure can then be used to determine from one local user identity a corresponding local user identity in a different user registry. The identity mapping mechanism thus allows user information in one environment to automatically retrieve user information in a different environment, thereby avoiding the necessity of the user remembering multiple usernames and passwords. Once a user it authorized to the network, and requests access to a resource, the security semantics

> for obtaining access to the resource may be satisfied by invoking the appropriate EIM APIs and submitting the appropriate security information.

That is, Botz at column 14, lines 23-34 discloses a user requesting access to a resource. Botz's user requesting access to a resource does not disclose receiving security information further comprises receiving a request for security information for the second security domain, wherein the request encapsulates the security information in a native format of a first security domain, as claimed in the present application, because Botz's request for a resource is not a request for security information for the second security domain. In contrast to a request for security information for the second security domain, Botz' request is for a resource. As discussed above, Botz does not disclose 'security domains.' Without disclosing security domains, Botz cannot disclose receiving security information further comprises receiving a request for security information for the second security domain, wherein the request encapsulates the security information in a native format of a first security domain, as claimed in the present application. Because Botz does not disclose each and every element and limitation of Appellants' claim 2, Botz does not anticipate Appellants' claim, and the rejections under 35 U.S.C. § 102 should be withdrawn.

The Office Action takes the position that Botz at figures 16-21 discloses the following limitation recited in dependent claim 6 of the present application: translating the security information in a native format of a first security domain to a canonical format is carried out through a procedural software function. Appellants note in response, however, that what Botz at figures 16-21 in fact discloses is block diagrams showing APIs that are included in the EIM ("Enterprise Identity Mapping") APIs ("Application Programming Interfaces"). Botz's APIs that are included in the EIM do not disclose translating the security information in a native format of a first security domain to a canonical format is carried out through a procedural software function. In the original specification, Appellants at page 15, line 31 – page 16, line 2, define a canonical format as a "data format for security information that is standardized for use in data transformations of security information." In contrast to security information that is translated from one

format to a data format that is standardized for use in data transformations of security information. In fact, at no point in the reference does Botz discuss the topic of translating data formats or even mention the keyword "canonical." Without disclosing translating data formats, Botz does not disclose translating the security information to a canonical format for security information is carried out through a procedural software function, as claimed in the present application. Because Botz does not disclose each and every element and limitation of Appellants' claims, Botz does not anticipate Appellants' claims, and the rejections under 35 U.S.C. § 102 should be withdrawn.

Relations Among Claims

Claims 3 and 6 recites method aspects for cross domain security information conversion according to embodiments of the present invention. Claims 12 and 21 respectively claim system and computer program product aspects corresponding to claim 3. Claims 15 and 24 respectively claim system and computer program product aspects corresponding to claim 6. Claims 3 and 6 are allowable for the reasons set forth above. Claims 12 and 21 are allowable for the same reasons that claim 3 is allowable. Claims 15 and 24 are allowable for the same reasons that claim 6 is allowable. The rejections of claims 12, 15, 21, and 24 therefore should be withdrawn, and claims 12, 15, 21, and 24 should be allowed.

Argument Regarding The Third Ground Of Rejection On Appeal: Claims 7-9, 16-18, 25-26, and 28 Are Rejected Under 35 U.S.C. 103(a) As Being Unpatentable Over Botz In View Of Bussler

Claims 7-9, 16-18, 25-26, and 28 stand rejected for obviousness under 35 U.S.C. § 103 as being unpatentable over Botz in view of Bussler, *et al.* (U.S. Patent No. 7,072,898). The question of whether Appellants claims are obvious or not is examined in light of: (1) the scope and content of the prior art; (2) the differences between the claimed invention and the prior art; (3) the level of ordinary skill in the art; and (4) any relevant secondary considerations, including commercial success, long felt but unsolved needs, and failure of others. *KSR Int'l Co. v. Teleflex Inc.*, No. 04-1350, slip op. at 2 (U.S. April 30, 2007).

Although Appellants recognize that such an inquiry is an expansive and flexible one, the Office Action must nevertheless demonstrate a prima facie case of obviousness to reject Appellants claims under for obviousness under 35 U.S.C. § 103(a). *In re Khan*, 441 F.3d 977, 985-86 (Fed. Cir. 2006). To establish a prima facie case of obviousness, the proposed combination of the references must teach or suggest all of the claim limitations of dependent claims 7-9, 16-18, 25-26, and 28. *In re Royka*, 490 F.2d 981, 985, 180 USPQ 580, 583 (CCPA 1974). Dependent claims 7-9, 16-18, 25-26, and 28 depend from independent claims 1, 10, and 19 and include all the limitations of the independent claims from which they depend. In rejecting dependent claims 7-9, 16-18, 25-26, and 28, the Office Action relies on Botz as disclosing each and every element of independent claims 1, 10, and 19. As shown above, Botz in fact does not disclose each and every element of independent claims 1, 10, and 19. Moreover, Bussler does not cure the deficiencies of Botz in disclosing each and every element and limitation of independent claims 1, 10, and 19. Because Botz does not disclose each and every element of independent claims 1, 10, and 19 and because Bussler does not cure the deficiencies of Botz, the combination of Botz and Bussler cannot possibly disclose each and every element of dependent claims 7-9, 16-18, 25-26, and 28. The proposed combination of Botz and Bussler, therefore, cannot be used to establish a prima facie case of obviousness, and the rejections 35 U.S.C. § 103(a) should be withdrawn.

In addition to Botz and Bussler not disclosing each and every limitation of the independent claims, the combination of Botz and Bussler also does not disclose the other limitations of Appellants dependent claims. Specifically, Appellants note that the combination of Botz and Bussler does not disclose the following limitations: mapping a system entity's identity in the first security domain to a another identity in the second security domain; receiving a request for security information for the second security domain, wherein the request encapsulates the security information in a native format of a first security domain; translating the security information in a native format of a first security domain to a canonical format is carried out through a procedural software function; the native format of the first security domain is expressed in XML, the canonical format is expressed in XML, and translating the security information in a

native format of a first security domain to a canonical format is carried out in dependence upon a mapping, expressed in XSL, from the native format of the first security domain to a canonical format; the canonical format is expressed in XML and the predefined mapping from the first security domain to a second security domain is expressed in XSL; and the second native format is expressed in XML, the canonical format is expressed in XML, and translating the transformed security information in the canonical format to a native format of the second security domain is carried out in dependence upon a predefined mapping, expressed in XSL, from the canonical format to the native format of the second security domain.

Conclusion of Appellants' Arguments

The Office Action rejects claims 10-28 under 35 U.S.C. § 101 as being directed to non-statutory subject matter. As explained above, Appellants' claims 10-28 are directed toward statutory subject matter entitled to patent protection under 35 U.S.C. § 101. Appellants therefore respectfully traverse the rejection and request reconsideration of claims 10-28.

Claims 1-6, 10-15, 19-24, and 27 stand rejected under 35 U.S.C. § 102 as being anticipated by Botz. Botz does not disclose each and every element of Appellants' claims and does not enable Appellants' claims. Botz therefore does not anticipate Appellants' claims. Claims 1-6, 10-15, 19-24, and 27 are therefore patentable and should be allowed. Appellants respectfully request reconsideration of claims 1-6, 10-15, 19-24, and 27.

Claims 7-9, 16-18, 25-26, and 28 stand rejected under 35 U.S.C. § 103 as obvious over Botz in view of Bussler. The combination of Botz and Bussler does not teach or suggest each and every element of Appellants' claims. Claims 7-9, 16-18, 25-26, and 28 are therefore patentable and should be allowed. Appellants respectfully request reconsideration of claims 7-9, 16-18, 25-26, and 28.

In view of the arguments above, reversal on all grounds of rejection is requested.

The Commissioner is hereby authorized to charge or credit Deposit Account No. 09-0447 for any fees required or overpaid.

Respectfully submitted,

Date: September 8, 2008 By: 

H. Artoush Ohanian
Reg. No. 46,022
Biggers & Ohanian, LLP
P.O. Box 1469
Austin, Texas 78767-1469
Tel. (512) 472-9881
Fax (512) 472-9887
ATTORNEY FOR APPELLANTS

APPENDIX OF CLAIMS
ON APPEAL IN PATENT APPLICATION OF
MATTHEW PAUL DUGGAN, *ET AL.*, SERIAL NO. 10/815,213

CLAIMS

What is claimed is:

1. A method for cross domain security information conversion, the method comprising:

receiving from a system entity, in a security service, security information in a native format of a first security domain regarding a system entity having an identity in at least one security domain;

translating the security information to a canonical format for security information;

transforming the security information in the canonical format using a predefined mapping from the first security domain to a second security domain;

translating the transformed security information in the canonical format to a native format of the second security domain; and

returning to the system entity the security information in the native format of the second security domain.

2. The method of claim 1 wherein transforming the security information includes structure transformation and value transformation, including mapping a system entity's identity in the first security domain to a another identity in the second security domain.

3. The method of claim 1 wherein receiving security information further comprises receiving a request for security information for the second security domain, wherein the request encapsulates the security information in a native format of a first security domain.

4. The method of claim 3 wherein the system entity comprises a system entity requesting access to a resource in the second security domain.

5. The method of claim 3 wherein the system entity comprises a system entity providing access to a resource in the second security domain.

6. The method of claim 1 wherein translating the security information in a native format of a first security domain to a canonical format is carried out through a procedural software function.

7. The method of claim 1 wherein the native format of the first security domain is expressed in XML, the canonical format is expressed in XML, and translating the security information in a native format of a first security domain to a canonical format is carried out in dependence upon a mapping, expressed in XSL, from the native format of the first security domain to a canonical format.

8. The method of claim 1 wherein the canonical format is expressed in XML and the predefined mapping from the first security domain to a second security domain is expressed in XSL.

9. The method of claim 1 wherein the second native format is expressed in XML, the canonical format is expressed in XML, and translating the transformed security information in the canonical format to a native format of the second security domain is carried out in dependence upon a predefined mapping, expressed in XSL, from the canonical format to the native format of the second security domain.

10. A system for cross domain security information conversion, the system comprising:

means for receiving from a system entity, in a security service, security information in a native format of a first security domain regarding a system entity having an identity in at least one security domain;

means for translating the security information to a canonical format for security information;

means for transforming the security information in the canonical format using a predefined mapping from the first security domain to a second security domain;

means for translating the transformed security information in the canonical format to a native format of the second security domain; and

means for returning to the system entity the security information in the native format of the second security domain.

11. The system of claim 10 wherein means for transforming the security information includes means for structure transformation and value transformation, including means for mapping a system entity's identity in the first security domain to a another identity in the second security domain.

12. The system of claim 10 wherein means for receiving security information further comprises means for receiving a request for security information for the second security domain, wherein the request encapsulates the security information in a native format of a first security domain.

13. The system of claim 12 wherein the system entity comprises a system entity requesting access to a resource in the second security domain.

14. The system of claim 12 wherein the system entity comprises a system entity providing access to a resource in the second security domain.

15. The system of claim 10 wherein means for translating the security information in a native format of a first security domain to a canonical format comprises a procedural software function.

16. The system of claim 10 wherein means for translating the security information in a native format of a first security domain to a canonical format comprises a mapping, expressed in XSL, from the native format of the first security domain to a canonical format.

17. The system of claim 10 wherein the canonical format is expressed in XML and the predefined mapping from the first security domain to a second security domain is expressed in XSL.

18. The system of claim 10 wherein the second native format is expressed in XML, the canonical format is expressed in XML, and means for translating the transformed security information in the canonical format to a native format of the second security domain comprises a predefined mapping, expressed in XSL, from the canonical format to the native format of the second security domain.

19. A computer program product for cross domain security information conversion, the computer program product comprising:

a recording medium;

means, recorded on the recording medium, for receiving from a computer program product entity, in a security service, security information in a native format of a first security domain regarding a computer program product entity having an identity in at least one security domain;

means, recorded on the recording medium, for translating the security information to a canonical format for security information;

means, recorded on the recording medium, for transforming the security information in the canonical format using a predefined mapping from the first security domain to a second security domain;

means, recorded on the recording medium, for translating the transformed security information in the canonical format to a native format of the second security domain; and

means, recorded on the recording medium, for returning to the computer program product entity the security information in the native format of the second security domain.

20. The computer program product of claim 19 wherein means, recorded on the recording medium, for transforming the security information includes means, recorded on the recording medium, for structure transformation and value transformation, including means, recorded on the recording medium, for mapping a system entity's identity in the first security domain to a another identity in the second security domain.

21. The computer program product of claim 19 wherein means, recorded on the recording medium, for receiving security information further comprises means, recorded on the recording medium, for receiving a request for security

information for the second security domain, wherein the request encapsulates the security information in a native format of a first security domain.

22. The computer program product of claim 21 wherein the computer program product entity comprises a computer program product entity requesting access to a resource in the second security domain.

23. The computer program product of claim 21 wherein the computer program product entity comprises a computer program product entity providing access to a resource in the second security domain.

24. The computer program product of claim 19 wherein means, recorded on the recording medium, for translating the security information in a native format of a first security domain to a canonical format comprises a procedural software function.

25. The computer program product of claim 19 wherein means, recorded on the recording medium, for translating the security information in a native format of a first security domain to a canonical format comprises a mapping, expressed in XSL, from the native format of the first security domain to a canonical format.

26. The computer program product of claim 19 wherein the canonical format is expressed in XML and the predefined mapping from the first security domain to a second security domain is expressed in XSL.

27. The computer program product of claim 19 wherein means, recorded on the recording medium, for translating the transformed security information in the canonical format to a native format of the second security domain comprises a procedural software function.

28. The computer program product of claim 19 wherein the second native format is expressed in XML, the canonical format is expressed in XML, and means, recorded on the recording medium, for translating the transformed security information in the canonical format to a native format of the second security domain comprises a predefined mapping, expressed in XSL, from the canonical format to the native format of the second security domain.

APPENDIX OF EVIDENCE ON APPEAL IN PATENT APPLICATION OF MATTHEW PAUL DUGGAN, *ET AL.*, SERIAL NO. 10,815,213

This is an evidence appendix in accordance with 37 CFR § 41.37(c)(1)(ix).

There is in this case no evidence submitted pursuant to 37 CFR §§ 1.130, 1.131, or 1.132, nor is there in this case any other evidence entered by the examiner and relied upon by the Appellants.

RELATED PROCEEDINGS APPENDIX

This is a related proceedings appendix in accordance with 37 CFR § 41.37(c)(1)(x). There are no decisions rendered by a court or the Board in any proceeding identified pursuant to 37 CFR § 41.37(c)(1)(ii).